WHAT IS CLAIMED IS:

1. In a public key authentication system, a method of sending an authenticated message to a recipient via a network, the method comprising:

digitally signing a message using a first private key associated with the sender;

retrieving a first certificate reference associated with a first certificate, the first certificate including a first public key corresponding to the first private key, wherein the first certificate and the associated first certificate reference are stored in a public key infrastructure; and

transmitting to the recipient via the network an authenticated message comprising the digitally signed message and the first certificate reference.

2. The method of claim 1, further comprising:

transmitting the first certificate via the network to the public key infrastructure prior to transmitting the authenticated message.

3. The method of claim 1, wherein the first certificate reference is determined from an identity of the sender and a serial number of the first certificate.

4. The method of claim 1 further comprising:

retrieving a second certificate reference to a second certificate, wherein the second certificate is issued to an issuer of the first certificate, wherein the second certificate and the associated second certificate reference are stored in the public key infrastructure; and

transmitting the second certificate reference as a further portion of the authenticated message.

5. The method of claim 1, wherein the network is the Internet.

6. The method of claim 1, further comprising encrypting the message using a second public key, wherein the recipient holds a second private key corresponding to the second public key.

7. In a public key authentication system, a method for authenticating a message received from a sender via a network, the received message including a digitally signed message and a first certificate reference, the method comprising:

transmitting the first certificate reference to a public key infrastructure via the network;

receiving from the public key infrastructure via the network a first certificate corresponding to the first certificate reference, the first certificate including a first public key;

determining whether the first certificate is trusted; and

if the first certificate is trusted, authenticating the digitally signed message using the first public key.

8. The method of claim 7, further comprising:

storing in a local keystore the first certificate reference and the first public key.

9. The method of claim 7, wherein the step of determining whether the first certificate is trusted comprises:

identifying a first issuer of the first certificate;

comparing the first issuer to each of at least one trusted issuer; and

if the first issuer is the same as one of the at least one trusted issuer, determining that the first certificate is trusted.

10. The method of claim 7, wherein the received message further includes a second certificate reference, the method further comprising:

transmitting the second certificate reference to the public key infrastructure via the network; and

receiving from the public key infrastructure a second certificate corresponding to the second certificate reference, the second certificate including a second public key associated with an issuer of the first certificate.

11. The method of claim 10, wherein the step of determining whether the first certificate is trusted comprises:

determining whether the second certificate is trusted;

if the second certificate is trusted, using the second public key to authenticate an issuer signature included in the first certificate, thereby verifying the first certificate; and

if the first certificate is verified, determining that the first certificate is trusted.

12. The method of claim 7, wherein the network is the Internet.

13. In a public key authentication system, a method for obtaining a public key for authenticating a received message comprising a digitally signed message and a first certificate reference, the method comprising:

determining whether the first certificate reference is stored within a local keystore;

if the first certificate reference is stored within the local keystore:

retrieving from the local keystore a first public key associated with the first certificate reference; and

if the first certificate reference is not stored within the local keystore:

transmitting the first certificate reference to a public key infrastructure;

receiving from the public key infrastructure a first certificate corresponding to the first certificate reference, the first certificate including the first public key;

determining whether to trust the first certificate; and

adding information to the local keystore, the information including at least the first certificate reference and the first public key.

14. The method of claim 13, further comprising:

authenticating the digitally signed message using the first public key.

15. A method of operating a public key infrastructure, the method comprising:

receiving a certificate from a first user;

computing a unique certificate reference from data contained in the certificate;

storing the certificate in association with the unique certificate reference;

receiving a request from a second user, the request including the unique certificate reference; and

transmitting the certificate to the second user in response to the request.

16. The method of claim 15, wherein the data contained in the certificate includes a subject identity and a serial number, and wherein the unique certificate reference is computed from the subject identity and the serial number.

17. In a public key authentication system comprising a sender, a recipient, a public key infrastructure and a network, a method of authenticating a message sent by the sender to the recipient, the method comprising:

at the sender side:

digitally signing a message using a first private key belonging to the sender;

retrieving a first certificate reference associated with a first certificate, the first certificate including a first public key corresponding to the first private key, wherein the first certificate and the associated first certificate reference are stored in the public key infrastructure; and

transmitting a message comprising the digitally signed message and the first certificate reference to the recipient via the network; and

at the recipient side:

receiving the message;

transmitting the first certificate reference to the public key infrastructure via the network;

receiving the first certificate from the public key infrastructure via the network; and

authenticating the digitally signed message using the first public key.

18. A public key infrastructure comprising:

a data store containing at least one certificate, wherein each of the at least one certificate is associated with a different one of at least one certificate reference; and

a server coupled to the data store,

wherein the server is configured to receive a certificate, to compute a certificate reference for the received certificate from data included in the certificate, and to store the received certificate in association with the computed certificate reference in the data store, and

wherein the server is further configured to respond to a request for a certificate, the request including a received certificate reference, by identifying and providing the one of the at least one stored certificate associated with the received certificate reference.

19. An electronic communication system comprising:

a public key infrastructure configured to store a plurality of certificates, to associate with each of the plurality of certificates a different one of a plurality of certificate references, and in response to a request including one of the plurality of certificate references, to return the corresponding one of the plurality of certificates;

a sender configured to digitally sign a message using a first private key and to send a message including the digitally signed message and a first certificate reference; and

a recipient configured to receive the message, to send a request including the first certificate reference to the public key infrastructure, to receive a corresponding first certificate from the public key infrastructure, and to use the first certificate to authenticate the digitally signed message.